ランサムウェア攻撃のアクター 特定をすべきこれだけの理由

一般社団法人JPCERTコーディネーションセンター
政策担当部長 兼 早期警戒グループマネージャ
脅威アナリスト
佐々木 勇人

前提：（パブリック）アトリビューションの「粒度」

- 「粒度」の異なる様々なアトリビューションと公表が行われている
- “ソフト”なアトリビューション：バーチャルな「攻撃グループ」の分類←セキュリティアナリストが行っているもの
- “ハード”なアトリビューション：実行犯／背景主体の特定←行政機関等で行っているもの

背後関係（所属組織、政府）
まで特定しているもの

実行犯（人物）特定まで
至っているもの

「攻撃グループ」特定
（+関係のある国／地域）

Sandworm

- ・ロシアのAPTグループと推測・特定されている
- ・2020/10にGRU要員の刑事訴追を公表

Lazarus

- ・北朝鮮のAPTグループと推測・特定されている
- ・2018/9, 2021/2に関係者の刑事訴追を公表

APT1

- ・中国のAPTグループと推測・特定されている
- ・2013/1にマンディアント社が実行者まで特定
- ・2014/5に米司法省が刑事訴追を公表

Kimsuky

- ・北朝鮮のAPTグループと推測されている
- ・標的が主に韓国
- ・これまでに実行犯個人の特定や、背後関係（どの組織に所属しているか）は明らかになっていない

SideCopy

- ・パキスタンのAPTグループと推測されている
- ・標的がインド、アフガニスタンの組織
- ・「パキスタン」を明示するセキュリティベンダもいれば、明示しないベンダも

前提：アトリビューションの全体像

そのアクター、本当にランサムギャング？

- RaaS/アフィリエイトスキームやロシア/東欧系の犯罪者の関与が注目されているが、実際には正体不明な単独の攻撃グループやAPTグループ（あるいは過去にAPTキャンペーンを行っていたグループ）によるランサムウェア攻撃も多数発生している
- ビルダーのリークなどにより、必ずしも“有名どころ”のランサムウェアが用いられたからといってRaaS傘下のアクターでないケースもある
- 他方で、ランサムウェア攻撃のインシデント対応では復旧が優先され、原因特定やランサムウェア/攻撃者の特定まで分析がなされないケースが多い。
- また、ファーストレスポンドーのインシデント経験不足、ランサムウェア攻撃対応の知見不足もあり、正確な分析がなされない傾向にある

対応事例① : Robinhood Leaks

- 遅くとも2021年10月から活動
- Raasなのか、単独の攻撃グループなのか不明であったが、この前後で、同一攻撃グループによるとみられる、別のランサムウェア（ブランド）を用いた攻撃事案を確認。同一グループが偽の“リブランド”をしているのではないかと考えられた
- 過去には欧州の損保会社、アフリカのマーケティング会社、中国の製造業等、アメリカのソフトウェア企業等を幅広く狙う
- Thanosランサムの亜種を使用（Thanosビルダーを使用している可能性）
- 暗号化後の拡張子は、被害組織名の略称と思われる（被害毎に異なる拡張子を使う）
- Twitterアカウントは2022年1月に凍結。その後はGettrアカウントを使用している。過去には他のSNSを用いていたことも。Toxでのチャットへ誘導するケースもある
- 過去には窃取したデータ（の一部）をSNS上にリークしていたが、その後行わなくなった
- SSL-VPN製品の脆弱性（あるいは過去に漏えいした認証情報）の悪用により侵入すると思われる

検体の特徴からの特定

- 同じ特徴を持つ複数の検体がVT上に存在していた
- 「暗号化後の拡張子 = 標的組織の略称」という特徴から、標的となった組織／地域を推測

#Thanos #Ransomware new extension. **拡張子**
Ransom note;RESTORE_FILES_INFO.txt
Robin Hood was generous and gave me a \$ 5,000 discount 😊
@RobinHoodLeaks account suspended.
VT sample [virustotal.com/gui/file/f9533288e6a7279195902c8691d5f223c77015fa332b56a23aeecc3581c0cdbdb](https://www.virustotal.com/gui/file/f9533288e6a7279195902c8691d5f223c77015fa332b56a23aeecc3581c0cdbdb)

44 / 67

44 security vendors and no sandboxes flagged this file as malicious

F9533288e6a7279195902c8691d5f223c77015fa332b56a23aeecc3581c0cdbdb
UEO22:PYPd3t

assembly calls-writ detect-debug-environment direct-cpu-clock-access peers runtime-modules

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Comments

angel973 2 months ago
#Malware #Trojan-Ransom

GrujaRS 2 months ago
#Thanos #Ransomware new extension **拡張子**

perisk 2 months ago
NARUM: Ransomware; Extension: NARUM; Ransom note: RESTORE_FILES_INFO.txt

<https://twitter.com/GrujaRS/status/1484148716479172608>

Modification events

PID	Process	Operation	Key	Name	Value
744	UEO22:PYPd3t.exe	write	HKEY_CURRENT_USER\Software\KEYID\myKeyID	ID1	
744	UEO22:PYPd3t.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	LegalNotice\Caption	YOUR COMPANY IS HACKED AND COMPROMISED
744	UEO22:PYPd3t.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	LegalNotice\Text	
744	UEO22:PYPd3t.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	legalnoticecaption	YOUR COMPANY IS HACKED AND COMPROMISED
744	UEO22:PYPd3t.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	legalnotice\text	
744	UEO22:PYPd3t.exe	write	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\FileSystem	LongPathsEnabled	1
744	UEO22:PYPd3t.exe	write	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	ProxyBypass	1
744	UEO22:PYPd3t.exe	write	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	IntranetName	1
744	UEO22:PYPd3t.exe	write	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	UNCASintranet	1
744	UEO22:PYPd3t.exe	write	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	AutoDetect	0

<https://any.run/report/f9533288e6a7279195902c8691d5f223c77015fa332b56e23aeecc3581c0cdbdb/ba082576-c0a4-4f18-9966-4b5e6da6108f>

Thanosビルダーを使用するランサムアクター

交渉手段／使用メディアからの特定

- 端末側のランサムノートに記載された2つのTox ID
BC6934E2991～
671263E7BC0～
- 同じTox ID記載のランサムノートが表示される検体について、一部ベンダが「JS Ransomware」と区分しているが、RobinhoodLeaksが用いるThanos亜種と思われる

EnigmaSoft

Home Products Malware Research Support Company

Home > Threat Database > Ransomware > JS Ransomware

JS Ransomware

By CagedTech in Ransomware

Translate To: English

Download

Not Your OS? Do...

* Free Remover allows you, subject to a 48-hour Read our [EULA](#), [Privacy/Cookie Policy](#) & [Disclaimer](#).

JS Ransomware Description

The JS Ransomware is a serious malware devices. Certain characteristics of the three corporate targets but the attackers could

| You have convinced me! |

Then you need to CONTACT US, there is few ways to DO that.

---Secure method---

a) Download a qTOX client: `hxps://tox.chat/download.html`

b) Install the qTOX client and register account

c) Add our qTOX ID:
BC6934E2991F5498BDF5D852F10EB4F7E1459693A2C1EF110266E5A259BBA3593769D766A275

or qTOX ID:
671263E7BC06103C77146A5ABB802A63F53A42B4C4766329A5F04D2660C99A3611635CC36B3A

d) Write us extension of your encrypted files .JS

Our LIVE SUPPORT is ready to ASSIST YOU on this chat.

40 security vendors and 1 sandbox flagged this file as malicious

94cdf8702480c306d69ae9aabb9ed09ce7b84f0cea8c001b378791094db079

BLrUxWwUwX

122.50 KB Size 2022-02-22 07:26:36 UTC 1 month ago

assembly detect-debug-environment direct-cpu-clock-access

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware		ⓘ Trojan.MSIL.Basic & Gen		
ALYac		ⓘ Trojan.MSIL.Basic & Gen		
Avast		ⓘ Win32.RansomX-gen [Ransom]		
Avira (no cloud)		ⓘ HEUR/AGEN.1235894		
BitDefenderTheta		ⓘ GenNN.ZemsiF.34232.hm0@Genroth		
Cyberession		ⓘ Malicious.342f68		
Cyren		ⓘ Malicious (score: 100)		
DrWeb		ⓘ Trojan.Encoder.NET29		
Emisoft		ⓘ Trojan.MSIL.Basic & Gen (B)		
ESET-NOD32		ⓘ A Variant Of MSIL/Filecoder.Thanos.A		
Fortinet		ⓘ MSIL.Thanos.Alt ransom		
Ikarus		ⓘ Trojan-Ransom.Thanos		

40 security vendors and 1 sandbox flagged this file as malicious

94cdf8702480c306d69ae9aabb9ed09ce7b84f0cea8c001b378791094db079

BLrUxWwUwX

assembly detect-debug-environment direct-cpu-clock-access peexe runtime-modules

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 2

Comments

pcrisk 29 days ago

JS Ransomware; Extension: .JS; Ransom note: RESTORE_FILES_INFO.txt

You must be signed in to post a comment.

攻撃インフラからの特定

37.143.131[.]224

2021/5/16~2022/2/10

※spookランサムの記事でも
確認されている

178.209.51[.]243

2021/8/4~2022/2/10

2022/2/10~

2022/2/10~

145.239.120[.]59

2022/2/10~

2021/8/4~2022/2/10

2020/8/27~2020/12/18

2021/8/26~

45.91.92[.]140

2020/3/31~2021/1/24

2020/8/27~2020/12/16

Validity 2022/2/9

Validity 2021/5/14

Validity 2020/3/30

Validity 2020/8/26

被害事案間の共通点

	Spookランサム事案	事案①	同事案②	同事案③
SSL-VPN製品	Fortigate ・2020/11 Fortifuckリストに該当はなし ・OSのバージョンは脆弱なまま	Sonicwall ・脆弱性のあるバージョンを使用 ・2021年にJPCERTからDC経由で通知	Sonicwall ・脆弱性のあるバージョンを使用 ・2021年にJPCERTからISP経由で通知	Fortigate ・2020/11 Fortifuckリストに該当あり ほか疑義のあるインフラが複数
SSL-VPNへの不正アクセス
拡張子	.spook	組織名の略称等を示す文字列		
ランサムノート（端末側）への連絡先記載		ToxのID	（未確認）	（未確認）
ランサムノート（サーバ側）への連絡先記載		（なし）	Twitterアカウント Gettrアカウント	Twitterアカウント Gettrアカウント

対応事例② : HUI loaderを用いる攻撃グループ

朝長 秀誠 (Shusei Tomonaga)

2022/05/16

HUI Loaderの分析

ツイート メール

攻撃者は、マルウェアの機能を隠蔽するために、マルウェア本体をエンコードし、実行時だけデコードして動作させることがあります。そのような場合、エンコードされたマルウェア本体は、ローダーと呼ばれるプログラムにロードされて、実行されます。このように、マルウェアをローダーとエンコードされたマルウェア本体に分割することで、ローダーの機能を最小限にし、マルウェアの重要な機能を隠蔽することで、感染ホスト上で発見することが難しくなります。今回は、このようなローダーの中で、2015年頃から使用されているHUI Loaderについて解説します。

HUI Loaderの概要

HUI Loaderについては、JSAC2022にて複数の攻撃グループによって使用されていることが指摘されていることが確認されています。JPCERT/CCでも、HUI Loaderを使用した攻撃を2015年頃から確認しています。図1は、HUI Loaderを使用した攻撃グループとHUI Loaderの変化を表したものです。

図1: HUI Loaderの変遷

JPCERT/CC Eyes 「HUI Loaderの分析」

<https://blogs.jpCERT.or.jp/ja/2022/05/HUILoader.html>

■ 侵入型ランサムウェア攻撃のインシデント対応でHUI Loaderを確認

■ HUI Loaderはもともと、さまざまな標的型サイバー攻撃グループが使用してきたもの

APT10 (2015年~)

Blue Termite (2015年~)

A41APT (2020年~)

DEV-0401 (2021年~)

```
push 0 ; lpName
push 0 ; dwMaximumSizeLow
push 0 ; dwMaximumSizeHigh
push 4 ; flProtect
mov esi, eax
push 0 ; lpMappingAttributes
push esi ; hFile
call ds:CreateFileMappingW
mov edi, eax
test edi, edi
jnz short loc_10002464
push eax ; Code
call _exit

-----
lea edx, [ebp+Buffer] ; CODE XREF: StartAddress+10C1j
push eax ; offset aHuihwasdihweiu ; "HUIHWASDIHWEIUDHDSFSEFPEWFEWDFSDGSEFERGW"
call _sprintf
add esp, 8
push 0 ; lpFileSizeHigh
push esi ; hFile
call ds:GetFileSize
push esi ; hObject
mov nSize, eax
call ds:CloseHandle
push 0 ; dwNumberOfBytesToMap
push 0 ; dwFileOffsetLow
push 0 ; dwFileOffsetHigh
push 4 ; dwDesiredAccess
push edi ; hFileMappingObject
call ds:MapViewOfFile
```

HUIローダーの特徴

- 2015年頃から、主に標的型サイバー攻撃での使用が確認されていたローダー
- 特徴的な文字列が検体内に内包されている

Japan Security Analyst Conference 2022 - カオス化する A41APT キャンペーン に対して私達ができること

HUI Loader の使用

- 2015年から存在していた名前の無いローダーが SodaMaster のローダーとして使用されていた
 - 文字列 "HUIHWASDIHWEIUDHDSFSFEFWFEWFDSDGFERFERWGWEFFWFEWD" から命名

```
Tuesday
Monday
Sunday
(null)
USER32.DLL
(((( H
h((( H
H
CONOUT$
HUIHWASDIHWEIUDHDSFSFEFWFEWFDSDGFERFERWGWEFFWFEWD
tna.conf
```

```
lea r8, aCWindowsInstall ; 'c:\\windows\\install.log
rcx, FileName ; lpFileName
db 66h, 66h, 66h, 66h
nop word ptr [rax+rax+00000000h]
mov eax, 'v'
lea rcx, [rbp+300h+Buffer] ; lpBuffer
mov [rsp+400h+filename+4], ax
mov eax, 'c'
mov edx, 104h ; uSize
mov [rsp+400h+filename+6], ax
mov eax, 'h'
mov dword ptr [rsp+400h+filename], 73005Ch ; "\s"
mov [rsp+400h+filename+8], ax
mov eax, 't'
mov dword ptr [rsp+400h+filename+0Ah], 73006Fh ; "os"
mov dword ptr [rsp+400h+filename+10h], 65002Eh ; ".e"
mov dword ptr [rsp+400h+filename+14h], 650078h ; "xe"
mov [rsp+400h+filename+18h], si
mov [rsp+400h+filename+0Eh], ax
call cs:GetSystemDirectoryW
xor eax, eax
```

28

https://jsac.jpCERT.or.jp/archive/2022/pdf/JSAC2022_9_yanagishita-tamada-nakatsuru-ishimaru_jp.pdf

DEV-0401

- 2021年以降に確認された「Lockfile」「AtomSilo」「Rook」「NightSky」「Pandora」の各ランサムウェアを用いた攻撃はすべて同一の攻撃グループ（「DEV-0401」（Microsoft社呼称名））によるものではないかと推測した。Microsoft社、SecureWorks社なども同様の指摘
- Microsoft社によれば、4月以降、Lockbit2.0をランサムウェアペイロードとして用いるようになってきているとの指摘。Sygnia社はCheercryptもDEV-0401の（偽装）“リブランド”によるものであると指摘。Secureworks社はAPT10との関連性を指摘。
- SSL-VPN経由で侵害せず、ProxyShell、Confluence脆弱性（CVE-2021-26084）、VMwareHorizonのLog4j脆弱性、ManageEngine ADSelfService Plusの脆弱性（CVE-2021-40539）などを初期侵入に悪用
- JPCERT/CCで確認した事案でもSSL-VPN経由のものは確認されず

出典：Microsoft <https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/>

Secureworks®

Next Intelligence Research | BRONZE STARLIGHT Ransomware Operations Use HUI Loader

THREAT ANALYSIS

BRONZE STARLIGHT Ransomware Operations Use HUI Loader

THURSDAY, JUNE 23, 2022
BY COGNATE THREAT INTELLIGENCE TEAM

Summary

Since at least 2021, threat actors have used HUI Loader to host remote access trojans (RATs) on compromised hosts. Secureworks® Cluster Threat Unit™ (CTU) researchers link two HUI Loader activity clusters exclusively to Chinese-based threat groups. The BRONZE STARLIGHT threat group is likely responsible for one cluster which focuses on stealing intellectual property from Japanese organizations. The other cluster involves deployment of Lockfile, AtomSilo, Rook, Night Sky, and Pandora post-infiltration ransomware. CTU researchers attribute this activity to the Chinese BRONZE STARLIGHT threat group.

The vestigial, often bypassed, step of each ransomware family, and access to malware used by government-sponsored threat groups suggest that BRONZE STARLIGHT's main motivation may be intellectual property theft or espionage rather than financial gain. The ransomware could distract incident responders from identifying the threat actors' true intent and reduce the likelihood of attributing the malicious activity to a government-sponsored Chinese threat group.

HUI Loader overview

HUI Loader is a custom DLL loader whose name is derived from a string in the loader (see Figure 1). The malware is loaded by legitimate programs that are vulnerable to DLL search order hijacking. HUI Loader originates and installs a threat file containing an encrypted payload that is also applied to the compromised host. CTU researchers have observed HUI Loader loading RATs, such as RemoteAccess, Phobos, Cobalt Strike, and Quantum.

出典：Secureworks
<https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader>

SYGNIA

PROACTIVE DEFENSE | ADVERSARIAL SECURITY | THREAT RESPONSE | VELOCITY XDR | RESOURCES

BACK TO RESOURCES

REVEALING EMPEROR DRAGONFLY: NIGHT SKY & CHEERSCRYPT - A SINGLE RANSOMWARE GROUP

出典：SYGNIA
<https://blog.sygnia.co/revealing-emperor-dragonfly-a-chinese-ransomware-group>

HUI Loaderを用いるDEV-0401の追跡

- Lockile、Atom Silo、Rookは、2021年9月にソースコードがリークしたBabukに類似
- NightSkyはRookに類似し、パッカーも同じ
- PandoraはRookとコードが重複しており、かつ、NightSkyとパッカーが同じ
- 各ランサム事案間のTTPも類似

使用したランサムウェア	LockFile	AtomSilo	Rook	Nightsky	Pandora	SecureWorks 対応事案
活動時期	2021年8月～	2021年9月～	2021年11月～	2021年12月～	2022年2月～	2022年2月
初期侵入	Proxyshell脆弱性	Confluence脆弱性 (CVE-2021-26084)	ManageEngine ADSelfService Plusの脆弱性 (CVE-2021-40539)が悪用された可能性	VMWare Horizon Log4j脆弱性		ManageEngine ADSelfService Plusの脆弱性 (CVE-2021-40539)
DLLサイドローディング	正規ファイルはKuGou Active Desktopを利用	正規ファイルはKuGou Active Desktopを利用		正規ファイルはマカフィー製品を利用	正規ファイルはマカフィー製品を利用	
HUI Loader	○	○	○	○	○	○
ランサム検体	← 類似 →			← 類似 →		
C2インフラ		NightSly事案と類似		Atomsilo事案と類似		

アクター特定が不十分なことで対応をしくじるケース①

- 国際情勢が緊迫度合いを増す中で、攻撃／攻撃の実行者を特定地域に紐づけたり、攻撃の動機／なぜ狙われたのかについて、国際情勢や“サプライチェーン”上の関係性に結び付ける憶測が飛び交う
- 実際は特定地域／サプライチェーンとはまったく関係のないアクターが行った、既知のランサムウェアを用いた攻撃であり、国際情勢が変化する前から活動していたものだったが、ある被害現場ではランサムウェア種別の特定まで誤認（攻撃グループX関連と紐づけてしまった）していたことが判明

アクター特定が不十分なことで対応をしくじるケース②

- あるマルウェア感染による通信が出ていた組織にコンタクトしたところ、1年以上前に発生したランサムウェア攻撃で使用されたマルウェアの“取りこぼし”によるものと判明
- 当時の調査ベンダは攻撃グループの特定ができておらず、この攻撃グループが当時多用していた初期侵入経路である脆弱なWebサーバの調査もしておらず、再発防止策も適切でないままだった

なぜ、ランサムウェアの攻撃グループ特定が必要なのか

- 初動対応を適切、速やかに、低コスト負担で行うため
 - 侵入原因の特定
 - 初動対応時から、用いられた攻撃手法を予想することで、 unnecessary NW遮断やフォレンジック等を減らせる
- 紛れ込んだAPTアクターを見逃さないため
- ランサムウェアの脅威の封じ込めを目指し、アクター毎に効果的な対抗措置を選択するため

目的：初動対応を速やかに、効率よく行うため

- ランサム種別・アクターの特定／絞り込みを行うことで、用いられたTTPsを推測する
 - 侵入経路・侵害拡大経路を絞り込み、調査の優先順位を決めることができる
 - 不要なNW遮断やシステム停止を可能な限り減らすことができる
- ・・・とはいえ、実際には「全台調査を」「情報漏えい有無の調査を」と求められる

なぜ個人情報漏えい有無の調査が優先されてしまうのか

- 個人情報保護法制度上の「速報」対応や被害個別通知対応に追われ、本来の事案対応リソースを消耗してしまっている

目的：身代金を支払わない合理的な判断のため

- 米主題のカウンターランサムウェア・イニシアティブ会合での声明など、各国において身代金支払いを制限する傾向
- アクターによっては、身代金支払い行為が制裁違反行為等に問われる恐れ
- とはいえ、「身代金は支払わないでください」だけでは判断できない
- 効率的な初動対応により、追加で発生してしまう“被害”を可能な限り低減する

目的：APTアクターの追跡・対抗のため

- 多くのLockbit2.0感染被害の中にAPT事案等が紛れており、これを見逃しているのではないか？

Lazarusのサブグループのケース

Cybersecurity Advisory TLP: CLEAR

Department of Homeland Security Cybersecurity Agency

#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

Summary

Note: This Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and various ransomware threat actors. These #StopRansomware advisories detail historically and recently observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn about other ransomware threats and no-cost resources.

The United States National Security Agency (NSA), the U.S. Federal Bureau of Investigation (FBI), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Department of Health and Human Services (HHS), the Republic of Korea (ROK) National Intelligence Service (NIS), and the ROK Defense Security Agency (DSA) (hereafter referred to as the "authoring agencies") are issuing this joint advisory.

- **Employ Various Ransomware Tools [TA0040]**. Actors have used privately developed ransomware, such as Maui and H0lyGh0st [T1486]. Actors have also been observed using or possessing publically available tools for encryption, such as BitLocker, Deadbolt, ech0raix, GonnaCry, Hidden Tear, Jigsaw, LockBit 2.0, My Little Ransomware, NxRansomware, Ryuk, and YourRansom [T1486]. In some cases, DPRK actors have portrayed themselves as other ransomware groups, such as the REvil ransomware group. For IOCs associated with Maui and H0lyGh0st ransomware usage, please see Appendix B.

https://media.defense.gov/2023/Feb/09/2003159161/-1/-1/0/CSA_RANSOMWARE_ATTACKS_ON_CI_FUND_DPRK_ACTIVITIES.PDF

DEV-0401

DEV-0401: China-based lone wolf turned LockBit 2.0 affiliate

Differing from the other RaaS developers, affiliates, and access brokers profiled here, DEV-0401 appears to be an activity group involved in all stages of their attack lifecycle, from initial access to ransomware development. Despite this, they seem to take some inspiration from successful RaaS operations with the frequent rebranding of their ransomware payloads. Unique among human-operated ransomware

China-based
DEV-0401 d
existing mal
heavily utili
vulnerabilit
Log4j 2, Du
elevated cre

Once inside
Cobalt Strik
preferences
frequently l
Impacket tool for WMI lateral movement, they use a customized version of the `wmiexec.py` module of the tool that creates renamed output files, most likely to evade static detections. Ransomware deployment is ultimately performed from a batch file in a share and Group Policy, usually written to the NETLOGON share on a Domain Controller, which requires the attackers to have obtained highly privileged credentials like Domain Administrator to perform this action.

Like many RaaS operators, DEV-0401 maintained a leak site to post exfiltrated data and motivate victims to pay, however their frequent rebranding caused these systems to sometimes be unready for their victims, with their leak site sometimes leading to default web server landing pages when victims attempt to pay. In a notable shift—possibly related to victim payment issues—DEV-0401 started deploying LockBit 2.0 ransomware payloads in April 2022. Around June 6, 2022, it began replacing Cobalt Strike with the Silver framework in their attacks.

DEV-0401 ransomware payloads over time

Figure 7. Ransomware payloads distributed by DEV-0401 between 2021 and April 2022

<https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/>

対抗措置例：アフィリエイトスキームのアクターの場合

- これまでもいくつかのアフィリエイトスキームが内紛等で消滅したり、関係者が逮捕されることで活動停止するなどした事例がある

対抗措置例：単独の攻撃グループの場合

- 偽の「リブランド」を行う理由 ⇒ 仮説：何らかの事情でアトリビューションされることを嫌う傾向／背景があるのではないか？
- （上記仮説に戻づくならば）実行犯の検挙等に至れなくても、注意喚起や分析レポート公表等で攻撃手法をさらすことである程度のけん制効果が出る可能性
- （アフィリエイトスキームに比べ、活動規模が大ききくはないため、（注意喚起等により）成功率／収益率をある程度低下させれば、致命的なダメージになる可能性。

対抗措置例：APTグループの場合

- これまでもパブリックアトリビューションで活動を停止／変化させたり、注意喚起や分析レポートで活動・手口を変えてきたAPTアクターが多いところ、同じような対抗措置や牽制や有効である可能性
- ランサムウェア攻撃はあくまで「副業」であるので、ある程度失敗が続けば一時的にランサムウェア攻撃から手を引いたり、あるいは無理に活動を継続しないのではないかと

まとめ：なぜ、ランサムウェアの攻撃グループ特定が必要なのか

- 初動対応を適切、速やかに、低コスト負担で行うため
- 紛れ込んだAPTアクターを見逃さないため
- ランサムウェアの脅威の封じ込めを目指し、アクター毎に効果的な対抗措置を選択するため（この後解説）

⇒ランサムウェア攻撃における被害者側のインシデント対応負担を減らせれば、身代金支払いに傾く被害組織は減る

⇒アクター毎に適切な対抗措置を行えば、実行者の数／層を減らしていくことができるのではないか？